реализованными в ПС и ОС контролируемых объектов;

– агенты системы, функционирующие на контролируемых объектах (серверах) и взаимодействующие со стандартными средствами протоколирования, имеющими отношение к безопасности событий, реализованными в ОС контролируемых серверов;

– АРМ АБ, ПС которого обеспечивают возможность управления системой и анализа полученной информации.

Система централизованного контроля и аудита средств защиты ККС «Мираж» версии 1.01 обеспечивает:

– контроль и аудит средств разграничения доступа ОС Windows NT/2000;

– контроль и аудит стандартных средств разграничения доступа Unix-совместимых ОС по протоколу syslog;

– контроль и аудит расширенных средств разграничения доступа Unix-совместимых ОС;

– контроль и аудит средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов, средств разграничения доступа устройств коммутации кадров сетевых протоколов, средств межсетевого экранирования и сенсоров систем обнаружения сетевых атак по протоколу syslog;

– контроль и аудит средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов, средств разграничения доступа устройств коммутации кадров сетевых протоколов, средств межсетевого экранирования и сенсоров систем обнаружения сетевых атак по протоколу SNMP;

– контроль и аудит средств разграничения доступа СУБД ORACLE, функционирующей на любой платформе.

Анализ информации, принятой от объектов контроля, выполняется на СБ в реальном времени. В случае обнаружения критичных для безопасности событий имеется возможность оперативного оповещения администратора безопасности (через консоль АРМ администратора, e-mail, sms и т. п.).

Модульная структура ПС СБ позволяет легко расширять его возможности (например, путем обеспечения мониторинга различных серверов приложений, устройств, поддерживающих протокол SNMP и т. п.).

В случае использования в ККС системы централизованного управления сетевыми ресурсами (типа HP OpenView, SPECTRUM и т. п.) информация, получаемая СБ от устройств коммутации кадров и маршрутизации пакетов сетевых протоколов (по протоколу SNMP), может быть получена с сервера данной системы.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 3. НД ТЗИ 2.5-004-99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа. 4. Баранов А. В., Петренко С. А. Системная интеграция и безопасность компьютерных сетей. Защита информации. Конфидент. № 2, 2001. 5. Внутренний мир Unix: Пер. с англ./ Хейр Крис и др. – К.: Издательство «ДиаСофт», 1998. 6. Доценко С. М. Система сетевой безопасности от одного производителя: миф или реальность? Безопасность информации, № 3, 2000. 7. Лукацкий А. В. Безопасность корпоративной сети глазами специалистов. Экспресс Электроника, № 4, 1999. 8. В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. Безопасность компьютерных сетей на основе Windows NT – М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd.", 1998. – 304 с. 9. Oracle8 Concepts. Release 8.0. A58277-01. 10. Real Secure. Network Sensor User Guide. Internet Security Systems, 2000. 11. Richard Power. Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare. Computer Security Institute, 1995. 12. Spectrum Concepts Guide. Cabletron Systems, 1996.

УДК 621.391.7

СУЧАСНИЙ СТАН РОЗВИТКУ КОНЦЕПЦІЇ ВІДВІДНОГО КАНАЛУ ТА ЗАДАЧІ ПОДАЛЬШОГО РОЗВИТКУ КОДОВОГО ЗАХИСТУ

Галина Кривоножко
ВІТІ НТУУ "КПІ"

Анотація: **Обговорюється проблематика та сучасний стан теорії кодового захисту інформації у спеціальних телекомунікаційних системах. Розглядаються найважливіші задачі аналізу та синтезу систем з кодовим захистом інформації. Обґрунтовуються показники і критерії стійкості цих систем.**

Summary: **The paper is devoted to the problems and the modern state of the theory of the code protection of the information in the special telecommunication systems. The most important tasks for analysis and synthesis of the systems with the code protection of the information are considered. The security indices and criteria of these systems are proved.**
Ключові слова: **Криптографічні системи, стійкість, ймовірнісно-криптографічний підхід, криптосистеми з випадковим кодуванням.**

І Вступ

Найважливішою складовою частиною систем захисту інформації є *криптографічні системи* (КС), роль яких завдяки інтенсивному розвитку інформаційних технологій і успіхам криптографії постійно зростає. Криптографічні системи являють собою сукупність ключової системи (множини припустимих значень ключа і протоколів застосування криптоперетворень) і самого криптографічного перетворення на основі деяких обернених перетворень інформації [1]. Вид ключової системи і криптоперетворень визначають основні властивості криптосистем і, як наслідок, – ефективність функціонування систем захисту інформації.

Центральним поняттям для криптографії і криптографічних систем є ***стійкість,*** під якою розуміють здатність криптосистеми протистояти всіляким атакам на неї [2, 3]. Необхідною умовою ефективності рішення задач захисту інформації, а значить, і якості систем, у яких ця інформація захищається (системи захисту інформації (СЗІ), спеціальні телекомунікаційні системи (СТКС)), є стійкість застосовуваних у них криптосистем.

Сьогодні телекомунікаційні системи мають потребу в криптосистемах з високою стійкістю і конструктивними протоколами розподілу ключів, що відповідають сучасним потребам інформаційних технологій, які розвиваються та впроваджуються, проблемної орієнтації у рішенні задач захисту інформації, конкретності функціонального призначення й умов застосування.

Якісне поняття стійкості є досить простим, але одержання досконалих доказових оцінок стійкості для кожного конкретного шифру (криптосистеми) із практичною стійкістю – проблема невирішена. Це пояснюється тим, що дотепер немає необхідних для рішення такої проблеми результатів. Тому стійкість кожної конкретної криптосистеми оцінюється тільки шляхом усіляких спроб її розкриття і залежить від кваліфікації криптоаналітиків [4]. Строго математично до цього питання підійшов К. Шеннон. Він розглядав питання про стійкість із двох різних точок зору [5]: *теоретичної (безумовної) стійкості і практичної (умовної, обчислювальної) стійкості.*

Рішення питання про теоретичну стійкість, що ввів К. Шеннон, вносить ясність для криптографа-теоретика, але ставить дуже складні задачі перед криптографом-практиком: обсяг таємного ключа для створення теоретично стійкого шифру виходить неприпустимо великим для більшості використань, а по суті він має бути рівним обсягу інформації, що захищається. Це робить абсолютно стійкий шифр дуже дорогим і непрактичним.

К. Шеннон розглянув також і питання *практичної стійкості*: чи надійна система, якщо криптоаналітик має обмежений час і обмежені обчислювальні можливості для аналізу криптограм. Це компроміс між можливим і бажаним. Стійкість практичних шифрів має спиратися не на теоретичну неможливість їхнього розкриття, а саме на практичну складність такого розкриття. Таким чином, для доказу практичної стійкості криптосистеми, створеної й побудованої на деякому припущенні про обчислювальні ресурси криптоаналітика, необхідно довести відсутність швидкого алгоритму (у рамках визначеної обчислювальної моделі) для розкриття шифру. Оскільки фактично для всіх обчислювальних задач у даний час неможливо знайти оптимальний алгоритм рішення чи дати нетривіальну нижню границю часу його виконання, остільки ніхто дотепер не просунувся у доказі стійкості практичного шифру. З цієї причини аналіз стійкості практичних шифрів, як правило, базується на припущенні (звичайно, який не розголошується явно), що криптоаналітик має *обмежені алгоритмічні* знання чи, більш точно, що єдино доступними алгоритмами зламу шифру є опубліковані в літературі чи хоча б відомі в криптоаналітичному суспільстві (відомстві) алгоритми. Складність задачі (у рамках заданої обчислювальної моделі) при використанні обмеженої множини алгоритмів має назву *історичної складності*. Оптимальний алгоритм задає *властиву складність*. Історична складність криптографічної задачі з розробкою нових алгоритмів зменшується, а властива складність (для заданої обчислювальної моделі) є величина постійна, але її неможливо визначити.

Таким чином, можна констатувати.

1. Теорія Шеннона дозволяє створювати криптографічні системи з доказовою стійкістю:
   - системи з теоретичною (безумовною, абсолютною) стійкістю;
   - системи з практичною (умовною, обчислювальною) стійкістю.
2. Системи з теоретичною стійкістю на практиці можуть бути реалізовані обмежено у зв'язку з їх низькими експлуатаційними характеристиками (висока вартість, невелика інформаційна місткість).

3. Практично стійкі системи широко використовуються, але оцінка їхньої стійкості має риси ризику (теоретична недоведеність, історична, а не властива складність, постійна залежність від розвитку математики, обчислювальної техніки та інше).

Тобто, обчислювальна стійкість існуючих практичних криптосистем не доведена і навіть не доведене їхнє існування. Стійкість кожної практичної криптосистеми, яку називають доказово обчислювально стійкою, ґрунтується на недоведеній гіпотезі про обчислювальну складність деякої обчислювальної задачі.

Тому, незважаючи на те, що доказова обчислювальна складність поки залишається однією з найбільш важливих теоретичних і практичних проблем у криптології, усе гостріше встає проблема побудови практично припустимих криптосистем з інформаційно-теоретичною стійкістю.

У рамках рішення цієї проблеми в останні два десятиліття спостерігається інтенсивний розвиток нових технічних, технологічних і навіть ідеологічних платформ побудови криптосистем із безумовною стійкістю [6].

Для подальшого розуміння нагадаємо, що криптографія – це наука про методи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів [4]. Власне методом перетворення інформації і визначається вид криптосистеми, тобто підходи до побудови криптосистем можуть мати різні технічні й технологічні платформи, відмінні від традиційних навіть в ідеології побудови криптосистем.

В даний час одержали розвиток дві нові платформи (по суті це нові ідеології) побудови криптосистем із безумовною (теоретичною) стійкістю: *квантова криптографія* і *ймовірносно-криптографічний підхід.*

Квантова криптографія, як принципово нова криптографічна ідеологія, була введена в 1983 р. Беннетом, Брассаром, Брайдхортом і Уизнером [4, 7]. Через те, що стійкість відповідної криптосистеми заснована на принципі невизначеності квантової механіки, цей напрямок одержав назву *квантової криптографії* [8 – 10] і сьогодні інтенсивно розвивається.

Разом із тим слід зазначити, що квантово-механічний метод криптографічного перетворення орієнтований тільки на оптичне середовище поширення. Це до деякої міри звужує область його застосування, але анітрішки не применшує головного досягнення – об'єднання практичності й абсолютної стійкості.

Випадкова криптографія. У 1975 році була опублікована піонерська робота А. Вайнера, що поклала початок принципово новому підходу до криптографії, як до науки про методи перетворення інформації з метою її захисту [11]. Цей підхід отримав назви: концепція відвідного каналу (Wire-tap Channel, WTC), імовірнісно-кріптографічний підхід (ІКП), кодовий захист інформації (КЗІ).

Принциповим на сьогодні в цій концепції (як відомо авторам із досліджених публікацій) є те, що на основі її можливо будувати конструктивні криптографічні системи для практичного захисту інформації з теоретичною стійкістю. Ці системи отримали назву систем передачі з випадковим кодуванням (СПВК).

II Основні положення концепції Вайнера

Модель криптосистеми з випадковим кодуванням представлена на рис. 1.

Уперше така модель була розглянута у 1975 році в [11]. Запропонована схема представляє так званий погіршений широкомовний канал (ШК) з одним входом і двома виходами [12]. Проте на відміну від звичайної задачі максимізації швидкості передачі до обох одержувачів, традиційної для ШК, тут ставиться задача мінімізації кількості інформації, одержуваної незаконним користувачем, при зберіганні максимально можливої швидкості передачі інформації законному користувачу. З цією метою в [11] запропоновано здійснювати випадкове кодування на передачі і відповідне (не випадкове) декодування на прийомі.

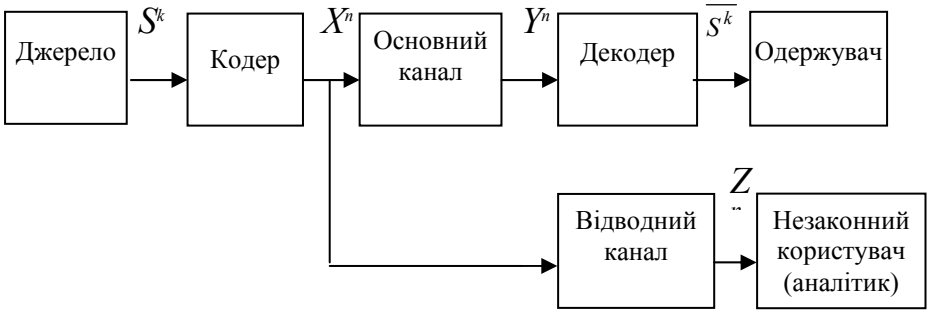

Рисунок 1 – Модель криптосистеми з випадковим кодуванням

Основними параметрами передачі в моделі, яка розглядається, є:

– швидкість передачі інформації – k/n;
– імовірність помилки на символ в основному каналі

$$P_e = \frac{1}{K}\sum_{i=1}^{K} p(s_i \neq s_{i'}); \tag{1}$$

– невизначеність інформації

$$\Delta = H(S^k \mid Z^n)/k\,. \tag{2}$$

Параметр Δ характеризує захищеність інформації щодо каналу відводу. Дійсно, використовуючи відоме співвідношення для кількості інформації, переданої каналом [13], можна записати

$$I(S^k; Z^n) = H(S^k) - H(S^k \mid Z^n), \tag{3}$$

де $H(S^k)$ – ентропія k-блоків джерела; $H(S^k \mid Z^n)$ – умовна ентропія джерела при відомих n-блоках на виході каналу; $I(S^k; Z^n)$ – середня взаємна інформація між k-блоками на вході і n-блоками на виході каналу.

Тоді очевидно, що якщо $H(S^k \mid Z^n) = H(S^k)$, то $I(S^k; Z^n) = 0$ і інформація незаконному користувачу не передається. Якщо $H(S^k \mid Z) = 0$, то $I(S^k;Z^n)=H(S^k)$ і незаконний користувач одержує повну інформацію про джерело. У проміжному випадку незаконний користувач одержує деяку кількість інформації, що відрізняється від нульової, але неповну.

Вищенаведене в повній мірі відповідає загальним основам побудови криптосистем з теоретичною стійкістю.

Розглянемо взаємозв'язок параметрів k/n, P_e, Δ при використанні асимптотично довгих кодів, тобто кодів з $n \to \infty$.

Відповідно до [11], пара чисел (R, d) називається досяжною для швидкості й непевності, якщо для будь-якого $\varepsilon \to 0$ існують кодер і декодер (f, φ), для яких

$$\frac{kH_\varepsilon}{n} \geq R - \varepsilon,\ \Delta \geq d - \varepsilon,\ P_\varepsilon \leq \varepsilon\,. \tag{4}$$

Область досяжних пар (R, d) позначимо через D.

В [11] доведена така фундаментальна теорема про характеризацію області D.

Т е о р е м а 1. *Область D досяжна тоді і тільки тоді, коли*

$$R \leq G_m,\ d \leq H_z,\ Rd \leq \Gamma(R), \tag{5}$$

де

$$\Gamma(R) = \max_{p(x)\in p} I(X,Y,|Z)\,, \tag{6}$$

p – множина розподілів ймовірностей $p(x)$ на вході каналу, для котрих $I(X;Y)\geq R$;

C_m – пропускна спроможність основного каналу $\{ X, p(y \mid x), Y \}$

Типовий вид області D показано на рис. 2.

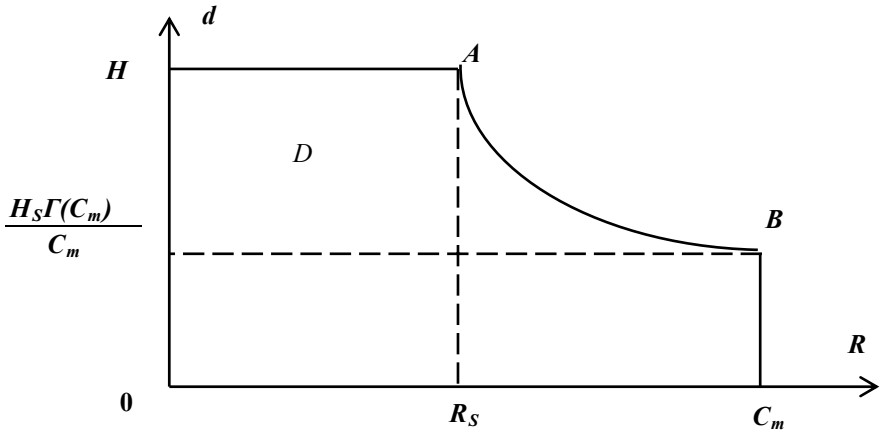

Рисунок 2 – Область досяжних швидкостей і непевності

Найбільший інтерес на цьому рисунку представляють дві точки: A – (R_S, H_S) і B – (C_m, d_B). Швидкість R_S є максимальною швидкістю передачі основним каналом, при якій каналом витоку інформації інформація взагалі не передається, тобто $H(S^k) = H(S^k \mid Z^n)$. Ця швидкість названа *секретною пропускною спроможністю.*

Точка B, для якої $R = C_m$, відповідає швидкості передачі, рівній пропускній спроможності основного каналу. Це максимальна швидкість, при якій можлива як завгодно надійна передача цим каналом ($P_e \to 0$, при $n \to \infty$). На цій швидкості передачі досяжна невизначеність $d_B = H_S\Gamma(C_m)/C_m$.

Основний висновок, що випливає з теореми 1, полягає в доказі існування засобу кодування-декодування для області кінцевих швидкостей передачі $0 \le R \le R_S$, при якому в каналі відводу може бути забезпечена як завгодно висока захищеність інформації $\Delta \to H_S$, якщо $n \to \infty$.

Для побудови стохастичного кодеру в [11] використовується кодова книга C, що являє собою множину підмножин C_i, $i = 1, 2, \ldots, M$, тобто

$$C = \bigcup_{i=1}^{M} C_i, \qquad C_i \cap C_j = \varnothing, \qquad i \ne j, \tag{7}$$

де M – число інформаційних k-блоків на вході кодеру.

Кожному інформаційному k-блоку $\overline{S}_j$ ставиться в однозначну відповідність одне з підмножин C_i, що містить M_1 n-блоків $\overline{x}$, а для передачі каналом випадково і рівно імовірно вибирається в цій підмножині слово $\overline{x}$. На прийомі декодування здійснюється шляхом зворотного перетворення, тобто відновлення інформаційного блоку $\overline{S}$, який відповідає підмножині C_i, що містить $\overline{x}$.

Найбільш складним при побудові області D є знаходження функції $\Gamma(R)$. Проте в деяких випадках вона є константою і знаходиться просто.

З того факту, що випадкові розміри X, Y, Z утворять марковську послідовність, випливає

$$\begin{aligned} I(X,Y \mid Z) &= H(X \mid Z) - H(X \mid Y,Z) = H(X \mid Z) - H(X \mid Y) = \\ &= I(X;Y) - I(X;Z). \end{aligned} \tag{8}$$

Достатні умови для того, щоб функція $\Gamma(R)$ була константою, містяться в теоремі 2 [14].

Т е о р е м а 2. *Нехай $I(X;Y)$ і $I(X;Z)$ одночасно максимізуються при деякому розподілі p_{x*}. Тоді $\Gamma(R)$ константа, яка рівна $C_m - C_{mw}$, де: C_{mw} – пропускна спроможність каналу $\{X, p(z|x), Z\}$.*

У цьому випадку секретна пропускна спроможність

$$R_S = C_m - C_{mw}. \tag{9}$$

З (8) випливає, що при фіксованій якості основного каналу збільшення R_S можливе за рахунок погіршення якості каналу відводу.

Для окремого випадку, коли основний і відвідний канали є двійковими симетричними каналами (ДСК), імовірність помилки в каналі відводу дорівнює p_w, а в основному каналі $p_m = 0$.

Якщо припустити, що джерело інформації безнадлишкове, тобто $H_S = 1$, то тоді справедлива наступна теорема.

Т е о р е м а 3. *Область D досяжна тоді і тільки тоді, коли*

$$0 \le R \le 1, \ 0 \le d \le 1, \ Rd \le h(p_w), \tag{10}$$

де

$$h(p_w) = -p_w \log p_w - (1 - p_w)\log(1 - p_w) \tag{11}$$

– ентропійна функція.

Очевидно, що умови теореми 2 виконуються, тому теорема 3 легко доводиться як наслідок теореми 1 заміною

$$C_m = 1, C_w = 1 - h(p_w). \tag{12}$$

Безпосередній доказ теореми приведено в [11].

III Сучасний стан розвитку

Розглянуті вище положення складають суть нової концепції перетворень для захисту інформації, що відрізняється від традиційної тим, що кінцева мета досягається не за рахунок яких-небудь секретних даних (ключів) або обміну захищеності на енергетичні параметри, а в результаті використання імовірнісного кодування.

Розглянуті результати відносяться до асимптотично довгих кодів, через що вони мало конструктивні. Не дослідженими є такі важливі питання, як критерії й оцінки захищеності інформації при використанні для кодового захисту кодів кінцевої довжини, конструктивні алгоритми кодування-декодування, оцінки ефективності такого захисту і їхнє експериментальне підтвердження, системно-технічний аналіз і технічні пропозиції з побудови проблемно-орієнтованих систем із імовірнісно-криптографічним кодуванням.

Найбільш важливі наукові і практичні результати, в яких відображена сутність наукової й технічної проблеми, що вирішується, полягає в наступному.

1. Розроблено науково-технічні основи конструктивної побудови систем захисту інформації і їхніх елементів на основі кодового захисту, що забезпечують високу ефективність захисту інформації з безумовною стійкістю криптографічних перетворень в інформаційно-теоретичному сенсі.

Розроблені науково-теоретичні основи включають наступні аспекти:

- концептуальні основи побудови й стійкість ймовірносно-криптографічних систем;
- синтез конструктивних алгоритмів побудови систем і засобів кодового захисту з не експоненціальною складністю;
- методологію оцінювання ефективності систем і засобів кодового захисту для реальних джерел інформації і не асимптотичних кодів;
- методологію побудови проблемно-орієнтованих систем і засобів із кодовим захистом інформації;

2. Запропоновано і введено сукупність показників і критеріїв захищеності інформації при кодовому захисті для реальних джерел. Уведено три моделі джерел інформації (надлишкового, детермінованих повідомлень і унікальних повідомлень). Для кожної моделі джерела визначені інформаційні і імовірнісні показники й критерії захищеності при декодуванні сигналів у каналі відводу.

3. Для введених моделей джерел і критеріїв їхньої захищеності отримано аналітичні співвідношення, що дозволяють здійснювати розрахунок стійкості кодового захисту для ідеального основного каналу.

4. Здійснено розробку ряду конструктивних алгоритмів, що володіють не експоненціальною складністю реалізації. Алгоритми орієнтовані на апаратну і програмну реалізації.

Отримані в даний час наукові й практичні результати з розвитку концепції відвідного каналу підтверджують, що можливою є побудова криптосистем із теоретичною стійкістю і високою технічною ефективністю для цілого ряду проблемно-орієнтованих задач. Проте, у рішенні цих проблемно-орієнтованих задач на основі теорії кодового захисту існує серйозне обмеження: практично всі отримані результати стосуються ідеального основного каналу, що є окремим випадком.

В даний час поставлені і вирішуються наукові задачі, що дозволяють розвити теорію кодового захисту для проблемно-орієнтованих цілей у випадку не ідеального основного каналу.

Відповідно до поставленої цілі методологічні аспекти розв'язуваної задачі розбиваються на ряд складових взаємозалежних частин, що визначають основні напрямки досліджень і черговість виконання.

До числа таких напрямків відносяться:

- обґрунтування й вибір показників і критеріїв розрахунку стійкості імовірнісно-криптографічних перетворень у системах кодового захисту;
- синтез конструктивних алгоритмів реалізації випадкового кодування в суміжних класах із не експоненціальною складністю побудови кодера й декодера для випадку не ідеального основного каналу;
- методологія оцінки ефективності кодового захисту на не асимптотичних кодах для реальних джерел інформації і не ідеальних та статистично незалежних основному й відвідному каналах;
- експериментальна перевірка і практичне впровадження основних наукових результатів.

У напрямку розвитку КЗ у випадку не ідеального основного каналу отримано конструктивний алгоритм випадкового кодування в суміжних класах із не експоненціальною складністю реалізації, що відкриває можливість для подальших досліджень.

Література: 1. Месси Дж. Л. Введение в современную криптологию // ТИИЭР. – Т. 76. – 1988. – № 5. – С. 24–42. 2. Дориченко С. А., Ященко В. В. 25 Этюдов о шифрах // Математические основы криптологии. – М.: ТЭИС. – 1994. – 69 с. 3. Шеннон К. Работы по теории информации и кибернетике / Под ред. Р. Л. Добрушина и О. Б. Лупанова. – М.: Изд-во ин. лит-ры, 1963. – 829 с. 4. Maurer U. M. Provable Security in Cryptography. Dissertation for the degree of Doctor of Technical Scienus. Zurich, 1990. 5. Shannon C. E. (1949). Communication Theory of Secrecy System // Bell Syst. Tech. J. 28. – P. 657–715. 6. Горицкий В. М. Вероятностная криптография в системах защиты информации: кодовая защита. Электроника и связь, вып. № 5, 1998 г., с. 140–145. 7. Bennett C. H., Bessette F., Brassard G. Experimental Quantum Cryptography // Journal of Cryptology . – 1992. – P. 53–78. 8. C. Marand and P. D.Townsende. «Quantum Key Distribution Over Distance as long as 30 km», Optics Letters, 20 1659–1697, 1995. 9. R. J.Hudges, G. G. Luther, G. L. Morgan and C. Simmons. In Proceeding of the Seventh Rochester Conference on Coherence and Quantum Optics, Rochester, NY, 1995. 10. R. J. Hudges, G. G. Luther, G. L.Morgan and C.Simmons. «Quantum Cryptography over 14 km of Installed Optical Fibre» in Proceedings of the Seventh Rochester Conference on Coherence and Quantum Optics. 11. Wyner A. D. The Wire-tap Channel // Bell System. Tech. J. – V. 54. – 1975. – № 8. – P. 1355–1387. 12. Колесник В. Д., Полтырев Г. Ш. Курс теорії інформації. – М.: Наука, 1982. – 416 с. 13. Галлагер Р. Теория інформації і

надійний зв'язок. – М.: Сов. радіо, 1974. – 720 с. 14. Leung-Yan-Cheong S. K. On a Special Class of Wire-tap Channels // IEEE Trans. on Inform. Theory. – Vol. 24. – 1978. – № 4. – P. 268–275.

УДК 621.391.7

АВТЕНТИФІКАЦІЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницький державний технічний університет

Анотація: **Пропонується метод автентифікації, в основі якого лежить використання властивостей класу рекурентних послідовностей, для обчислення елементів яких використовуються рекурентні співвідношення з коефіцієнтами, що пов'язані з початковими елементами послідовностей.**
Summary: **The method of authentication is offered, in which base use of properties of the class recurrent of sequences lays, at calculation of which elements the recurrences with coefficients coupled to initial elements of sequences are used.**
Ключові слова: **Захист інформації, криптографія, автентифікація, рекурентні послідовності.**

I Вступ

В сучасному світі поняття "інформація" відіграє важливу роль. У різних своїх формах та проявах інформація стала товаром, який створюється, зберігається та передається користувачам, споживачам. Кожна інформація має свою ціну, а отже може продаватися та купуватися, старіти та пошкоджуватися і т. і. Найпоширенішими на сьогодні засобами для зберігання, обробки та передавання інформації є комп'ютерні системи, в яких інформація представляється в цифровому вигляді. Протягом всього циклу існування інформації однією з основних проблем для споживача є проблема її захисту від небажаного втручання та впливу з боку зловмисника. Для вирішення цієї проблеми в комп'ютерних системах застосовують криптографічні методи захисту інформації [1].

Історично криптографія виникла як наука про шифрування інформації, тобто як наука про криптосистеми [2]. В класичній шенонівській моделі [3] системи секретного зв'язку мають двох учасників, які повністю довіряють один одному і передають між собою інформацію, що не призначена для сторонніх осіб. Таку інформацію називають секретною або конфіденційною, а задачу, яка тут виникає, називають задачею забезпечення конфіденційності або секретності від зовнішнього противника [3]. Традиційно ця задача розв'язується за допомогою криптосистем.

Швидкі темпи розвитку засобів зв'язку та комп'ютерних мереж привели до широкого впровадження електронних банківських платежів та можливості обміну різного роду електронними документами. В зв'язку з цим у споживача можуть виникнути обґрунтовані сумніви відносно того, що отримана ним інформація створена потрібним джерелом, причому в такому вигляді, в якому вона дійшла до нього. Тобто необхідна гарантія того, що повідомлення надійшло з достовірного джерела та в неперекрученому вигляді. Така гарантія отримала назву забезпечення цілісності інформації [4] і складає другу задачу криптографії.

Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації розробляються криптографічні протоколи [2]. Найбільш розповсюдженими є два типи криптографічних протоколів: схеми автентифікації та цифрового підпису [4].

Схеми автентифікації використовуються для встановлення авторства (або ідентифікації). На цей час актуальність задачі автентифікації має не менше, а в деяких випадках і більше, значення, ніж задача конфіденційності інформації.

II Постановка задачі

В загальному вигляді в схемі автентифікації [2] існує два учасника. Передавач, який має довести свою автентичність, та Приймач, який цю автентичність має перевірити. Передавач має два ключа – загальнодоступний K_1 та секретний K_2. Передавачу необхідно довести, що він знає K_2, причому зробити це таким чином, щоб це доведення можна було б перевірити, знаючи лише K_1.

Найбільш відомими методами автентифікації з точки зору встановлення авторства повідомлення є методи Фейге-Фіата-Шаміра, Гіллу-Кіскатра та Шнорра [2]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його